No more sources? The impact of Snowden's revelations on journalists and their confidential sources.

Dr Paul Lashmar, Journalism, School of Media, Film and Media, Brighton, University of Sussex, UK. p.lashmar@sussex.ac.uk

No more sources? The impact of Snowden's revelations on journalists and their confidential sources.

From June 2013 documents leaked by the National Security Agency (NSA) dissident Edward Snowden revealed that Western intelligence agencies are capable of bulk collection of electronic communications flowing through global telecommunication systems. Surveillance data shared by the 'Five Eyes' eavesdropping agencies of the US, UK, Canada, Australia and New Zealand include journalist's communications. In the wake of Snowden leak, Zygmunt Baumann et al called for a systematic assessment of the scale, reach and character of contemporary surveillance practices (2014, 122). This paper explores a specific part of Bauman's task by assessing the impact of the Snowden revelations on confidential source-based journalism. Interviews were conducted with a range of investigative journalists who have experience of covering national security in Five Eyes countries. All expressed serious concern over the intelligence agencies' greatly enhanced capability to track journalists and identify and neutralise their sources. The paper concludes that there is clear evidence of a paradigmatic shift in journalist-source relations as those interviewed regard Five Eyes mass surveillance as a most serious threat to the fourth estate model of journalism as practiced in Western democratic countries.

Keywords: Investigative journalism; sources; source protection; five eyes; NSA; GCHQ; Snowden; National Security reporting

Note: All interviews are with the author unless otherwise referenced.

Introduction

The documents leaked to journalists in June 2013 by the whistle-blower and former National Security Agency (NSA) contractor Edward Snowden have revealed that western intelligence agencies have conducted, and continue to conduct, surveillance and metadata bulk collection on a vastly greater scale than previously suspected. The purpose of this paper is to establish whether government mass surveillance is impacting on the ability of journalists to establish and maintain sources. The then Editor of UK newspaper *The Guardian*, Alan Rusbridger, warned that this level of surveillance has serious implications for journalism: "Every journalist should understand that there is no such thing as confidential digital communication. None of us have confidential sources." He continued: "We are all going to have to work on this, in this world where people can intercept everything." Rusbridger said bulk collection is a direct threat to journalism, its practitioners and sources (Ponsford, 2014). The paper also discusses the importance of confidential sources to quality journalism and the democratic process. The author is an investigative journalist, more recently an academic, with several decades of experience in both national security reporting and working with confidential sources.

In media theory the enlightened and aspirational role of the news media in a liberal democracy is often characterised as that of the fourth estate where journalists are seen as the guardians of the public interest (Carlyle 1840). The fourth estate concept tasks the media to hold the errant, whether the state or the powerful, to account. The fourth estate model was challenged by other more nuanced and realistic models as early as 1923 when Robert Park (273) dismissed this model as overly simplified. "The press, as it exists, is not, as our moralists sometimes seem to assume, the wilful [sic] product of any little group of living men". However, as Professor Steve Barnett observed, a vigorous journalistic culture – in particular challenging investigative journalism – is vital for a healthy democracy. He said: "Without it, executive or corporate wrongdoing will not only continue but can eventually corrupt the body politic" (Allan 2005, 329). To fulfil this function journalists need confidential sources, individuals who provide public interest information, usually from within organisations (e.g. government).

Edward Snowden

Edward Snowden (born 1983) is an American computer specialist, a former Central Intelligence Agency (CIA) employee, and National Security Agency (NSA) contractor who established unauthorised contact with journalists Glenn Greenwald and Laura Poitras from late 2012. Since June 2013, a range of Snowden's leaked documents have been published by media outlets worldwide, most notably The *Guardian* (Britain), *Der Spiegel* (Germany), The *Washington Post* and The *New York Times* (US), *O Globo* (Brazil), *Le Monde* (France), and news outlets in Sweden, Canada, Italy, Netherlands, Norway, Spain, and Australia. Although only a small percentage of Snowden's estimated 1.7m documents have been published, these reveal operational details of a global surveillance apparatus jointly run by the Five Eyes in close cooperation with their commercial and international partners.[1] The Five Eyes is a partnership of the eavesdropping organisations of Australia (ASD), United Kingdom (GCHQ), United States (NSA), Canada (CSEC), and New Zealand (SIS). The US investigative journalist Seymour Hersh is certain that NSA whistle-blower Edward Snowden "changed the whole nature of the debate" about surveillance. Hersh said he and other journalists had written about surveillance, but Snowden was significant because he provided documentary evidence.

> Duncan Campbell [the British investigative journalist who broke the Zircon cover-up story], James Bamford [US journalist] and Julian Assange and me and the *New Yorker*, we've all written about the notion there's constant surveillance, but he [Snowden] produced a document and that changed the whole nature of the debate, it's real now (O'Carroll 2013).

Glenn Greenwald, the former *Guardian* journalist, who worked with Edward Snowden summarised his perception of the NSA's network's operation:

> It is now apparent that metadata[2] of most emails, many phone calls and much more is being copied into huge data stores that allow the agencies to sift for useful information. Snowden has also revealed that the agencies have secretly negotiated for "backdoors" in the security of many computer programmes, social networking sites, websites and smartphones (Greenwald 2013b).

Metadata collection is one of the methods the intelligence agencies use to surveil targets and can be applied to journalists, their sources or any other person. This paper does not seek to discuss details of the actual surveillance programmes nor the morality or legality of Snowden's decision to leak the material only the impact on journalism. The philosopher Zygmunt Bauman, working with Didier Bigo and others has attempted to characterise the considerable implications for nation states of the extra-national and domestic activities of intelligence agencies as revealed in Snowden's documents. "There is an urgent need for a systematic assessment of the scale, reach and character of contemporary surveillance practices, as well as the justifications they attract and the controversies they provoke" (Bauman et al 2014, 122). This paper is intended to go some way to meet Baumann's challenge.

Literature Review

This literature review began, in effect, with the contemporary reading in 1976 of CIA dissident Phillip Agee's biographical account of his work in "Inside the Company: CIA Diary" (Agee 1975).[3] Since, with one text leading to the next, in a "snowball" approach, the author had considered many of the texts published that feature in some regard, in full or in part, the intelligence world and also its relationship with the media. For this literature review the author also used the University library to identify all journal papers and books relevant to Snowden, journalism and sources.[4] Specifically included were Sigal 1973; Parrell 1993; Pearlstine 2007; Sager and Wilcox 2007 and Corera 2015. A number of books on the Snowden Affair were consulted including Harding 2014; Greenwald 2015 and, in terms of Surveillance studies, Lyon 2015. These readings have provided a comprehensive insight into the workings and development of intelligence agencies, especially those engaged in electronic espionage, and has given an impression of those agencies' efficacy and their relationship with power. This literature review seeks to set out the debate over journalism and sources, so that the likely impact of intelligence agencies' enhanced surveillance technology can be assessed.

Sources

Within journalism studies there has been a discourse about news sources and their role in the modern news media (Hall et al 1978; Gans 1980; Schlesinger 1994; Schlesinger and Tumber 1994; Cottle 1998; Manning 2001; Broersma et al 2013 and much discussion in other Five Eyes countries). These discussions set out a theoretical framework for how the

news media find, use and publish source material. Most sources are open but some are described as anonymous or confidential. These may or may not be referred to in the journalist's story but never by name. While critical of what he sees as the overuse of unnamed sources, Matt Carlson accepts that pushing aside attribution allows journalists to challenge on-the-record claims or force out into the open guarded information. "This revelatory perspective of unnamed sources allows journalism to break from its stale patterns to truly serve out its normative pledge of holding power accountable. And while this may sound overly normative, there are ample moments in which journalists have broken a news story of considerable political importance through the use of unnamed sources" (Carlson 2012, 6-7). There is little research in this area but a 1971 US survey revealed that 22.6% of stories in daily newspapers depended on regular anonymous sources and a further 11.6% depended on first-time sources. A 1985 survey of reporters indicated reliance on unnamed sources in 31.25% of their news stories (Parrell 1993, 48). Although the US press has tougher strictures on the use of anonymous sources than other western nations, one study found extensive used of unnamed sources in US national security reporting in major newspapers with 48% of executive branch sources and 32% of congressional sources unnamed (Hallin et al 1993, 759). It would not be presumptuous to suggest that with the ubiquitous rise of the professional government PR industry and the financial pressures on the news media since, that these percentages would be much lower today.

The confidential source

What is considered in this paper is a very specific type of information provider, the journalist's confidential source, and this requires clarity. The former editor-in-chief of *Time* magazine Norman Pearlstine has made a useful clarification between anonymous sources and confidential source: "As a reporter and an editor, I had distinguished between "anonymous sources," whose names we wouldn't use in a story, and "confidential sources," whose identity we might decide to protect even after litigating and losing." He adds: "Since reporters were supposed to be trying to get their sources to go on record whenever possible, it seemed axiomatic that the source had to ask for confidentiality. A reporter couldn't make a source "confidential" without the source's agreement" (Pearlstine 2007, 102).The key here is the level of authority the source has to speak to a journalist. It is one thing for a source to speak officially - usually from within an organisation - on the condition of anonymity. It is quite another if the source is providing information without official permission, but with the condition of total confidentiality required from the journalist. In the author's experience as an investigative journalist, confidential sources can vary greatly from providing key unique information to confirmation of information gathered elsewhere (see Lashmar 2013a). Interviewees for this paper observed that each story involving source/leak/whistle-blower permutations is unique, with its own dynamic and narrative.

There is a substantial debate about the role and legal position of the confidential source especially in the United States where it features widely in academic law texts (Parrell 1993; Sager and Wilcox 2007). The confidential source is still a relatively under-researched area in UK journalism studies with a few notable exceptions. Kiernan states that investigative journalism by its very nature is often heavily reliant on sources who wish their identity to remain anonymous or to be protected in some way:

> Without the promise of confidentiality which the source can trust in, investigative journalists would often be unable to get crucial information about scandals or substantiating corruption. Thus, once commitments are made they are heavily binding. If it were common practice for such commitments to be made and then

broken, sources would not trust journalists and reveal information to them (Kiernan 2000, 169).

Confidential sources can become whistle-blowers, but only a small proportion do. This paper does not attempt to consider whistle-blowers as that would make the scope too wide as protecting whistle-blowers has yet another series of legal issues for the journalist to consider.[5] This paper defines whistle-blowers as someone who goes public and/or are known to be a whistle-blower to the organisations that they are exposing.

Leaks

Leaks have been a feature of journalism from its earliest incarnations but the late Chapman Pincher is reputed to be the first UK journalist to master the art of the "exclusive by leak" from politicians and officials (see Moran, 2013; Pincher, 2009). Without rivalling Pincher's reputation, the author too, for most of his career, nurtured sources within law enforcement, intelligence and other public sector agencies and published many "in the public interest" stories from these sources. The author echoes other colleagues quoted in this paper to say it is vital that journalists can guarantee their sources' anonymity and employed a range of common sense approaches about communicating and anti-surveillance techniques for meeting and communicating that were effective. In consequence, protected insider sources helped, for instance, while the author was working for the *Independent on Sunday* (2001-2007), to understand that the leadership at MI6 had become political in providing "evidence" justifying the Iraq War (Whitaker et al 2003). In the fourth estate model the possibility of exposure by the journalists constrains policy makers and officials from acting against the public interest. If the flow of information from confidential sources were to cease, journalists would be hard put to meet their fourth estate role (see also Reich 2008). An interviewee for this paper, Australian journalist Dr Philip Dorling[6], observed that the possibility of leaks to journalists had a cautionary effect on officials and politicians as they knew there was a risk of exposure for any dissembling (Dorling 2012). This is a vital point.

Sources and ethics

The protection of sources is a core concept in the journalists' *habitus*. All the major ethical codes for journalists throughout the world cover source protection. The International Federation of Journalists (IFJ) Declaration of Principles on the Conduct of Journalists is clear on protecting Sources (IFJ 1986). In the UK there is the National Union of Journalists' (NUJ) Code of Conduct. As Crook observed, Article 7 of the code states a journalist shall protect confidential sources of information: "The obligation brooks no qualification. The duty is deontological. In philosophical terms this means that not protecting the source is *always* wrong" (Crook 2003, 8). The UK media commentator, Professor Tim Luckhurst, observed: "The legend of Deep Throat[7] runs deep and, to British journalists, it conveys a solitary absolute: confidential sources must never be identified while they are alive" (Luckhurst 2003). This duty applies equally in other countries and Australian journalist Andrew Fowler[8] observed: "Trying to protect source is the thing that you do. You don't want to harm a source. You will protect with your life, of course." Journalists have gone to prison rather than reveal their source's identify. The controversial *New York Times* journalist Judith Miller who had been fed stories by the Bush administration in favour of the Iraq invasion, Miller was also involved in the Plame Affair. Miller revealed that Valerie Plame was a member of the Central Intelligence Agency (CIA). When asked to name her sources, Miller invoked reporter's privilege and refused to reveal her sources and spent 85 days in jail.

In terms of the law in Europe, the European Court of Human Rights pronounced in the 1996 case of *Goodwin v. United Kingdom* that protection of journalistic sources is one of the basic conditions for press freedom:

> Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected.

The Court ruled that unless there was "an overriding requirement in the public interest" an order to disclose sources would conflict with the guarantee of free expression in Article 10 of the European Convention on Human Rights (ECHR 1996). While the laws of the Five Eyes countries recognise that journalists need to protect sources, the actual level of protection varies. On occasion the media themselves have failed to protect their sources provoking appropriate condemnation. In the UK in 1983 *The Guardian* controversially handed over documents to the Government that allowed the identification and prosecution of the Foreign Office clerical officer Sarah Tisdall. She, on a matter of personal principle, had anonymously sent *The Guardian* photocopies detailing when American cruise missile nuclear weapons would be arriving in Britain. The documents set out the political tactics Michael Heseltine, then Secretary of State for Defence, would use to present the matter in the House of Commons. She was sentenced to six months in prison. Since 2013 two British news companies handed to police the names and details of its journalists' sources in the public sector to whom the company had previously covertly paid "tip-off" fees. Payments to public officials were outlawed by the Bribery Act 2010. As a result more than 30 public officials have been convicted with many sent to jail. The Editor of the UK's Press Gazette Dominic Ponsford said that Rupert Murdoch's News Corp and Trinity Mirror group need to address betrayal of sources if the industry is to move on:

> Both companies have so far been silent on this issue. If we are to move on as an industry they need to reassert the fact that sources are sacrosanct and reveal what measures have been taken to ensure that such a betrayal of the first principle of journalism can never happen again (Ponsford 2015).

"Chilling Effect"

The idea that the ability of journalists to maintain confidential sources is important to the wellbeing of society is not a recent one. In the Watergate scandal Bob Woodward, Carl Bernstein, and eight other journalists were subpoenaed to disclose the sources of their information. In *Democratic Nat'l Comm. v. McCord, 356 F. Supp. 1394 (D.D.C. 1973)* the district court, after recognising the importance of the information obtained through confidential sources, rejected the subpoenas. It explained:

> This Court cannot blind itself to the possible "chilling effect" the enforcement of these broad subpoenas would have on the flow of information to the press, and so to the public. This Court stands convinced that if it allows the discouragement of investigative reporting into the highest levels of government, no amount of legal theorizing could allay the public's suspicions engendered by its actions and the matters alleged (Sager and Wilcox 2007).

The importance of journalists' confidential sources for monitoring the national security state – one of the most difficult arms of government for journalists to report - were yet again highlighted in 2006, when the Pulitzer Prize for National Reporting was shared by journalists

at two newspapers, one of which was the *New York Times*. Published on 15 December 2005 the story explained how "nearly a dozen current and former officials, who were granted anonymity because of the classified nature of the program, discussed it [the topic] with journalists for the *New York Times* because of their concerns about the operation's legality and oversight." The journalists were applauded for "their carefully sourced stories on secret domestic eavesdropping that stirred a national debate on the boundary line between fighting terrorism and protecting civil liberty." As Sager and Wilcox noted: "This story, like so many others, could not have been written without information from confidential sources" (2007: 41). There is a long history of the excesses of the national security state being revealed by journalists in all the Five Eyes countries.

Leak Inquiries

The state has always tried to minimise leaks usually by inquiries and prosecutions. In 1734, publisher John Peter Zenger refused to identify his source when prosecuted by colonial New York authorities for publishing articles critical of the royal government. His attorney, Andrew Hamilton, emphasised Zenger's protection of those who dared to criticize the government, describing his client as laying; "a noble foundation for securing **...** a right to liberty of both exposing and opposing arbitrary powers (in these parts of the world at least), by speaking and writing truth" (Sager and Wilcox 2007: 41). Canada, usually seen as a liberal nation, has seen a number of instances of the official pursuit of journalists and their sources. The most infamous if complex example concerns the Maher Arar affair. Arar was a telecommunications engineer with dual Syrian and Canadian citizenship. In 2002 suspected of being an al Qaeda member, he was arrested in JFK Airport and sent by the USA to Syria where he was tortured. Arar's story is frequently referred to as "extraordinary rendition' but the US government insisted it was a case of deportation. In 2003 Juliet O'Neill, a reporter with the *Ottawa Citizen*, wrote a 1,500-word story, citing anonymous intelligence sources and a document suggesting Mr Arar was a terrorist who had received training in a notorious camp for terrorists in Afghanistan. As a result on January 21 2004 the Royal Canadian Mounted Police (RCMP) raided her house as part of an attempt to identify the leak. During the raid, police seized notebooks, files, hard drives and other materials. The case became a freedom of the press issue. One of the interviewees for this paper, Canadian investigative reporter Andrew Mitrovica, took a different stance: "All the huffing and puffing about a 'police state' and 'dark' days for democracy emanating from CanWest's offices in Winnipeg and Ottawa might be a tad more plausible and genuine if the news service's reporters weren't playing footsie so blatantly with cops and/or spies," he stated (2005). Subsequently the Canadian courts ruled the raid was not justified. Mr Arar was eventually returned from Syria to Canada and exonerated (see Arar Inquiry 2006). Considering the US experience Sager and Wilcox, writing at the time of the Bush administration noted that:

> Journalists are more threatened today than at any time in American history. Never before have prosecutors, defendants, and civil litigants felt such freedom to demand that journalists produce confidential information. Never before have so many journalists been faced with the prospect of going to jail for refusing to comply with a disclosure order (2007, 42).

Barack Obama was critical of the national security state that emerged under George Bush but his administration has since greatly increased the pressure on journalists over their sources (Stein 2013). Another interviewee, the *New York Times* national security reporter, Scott Shane[9], noted that some intelligence agencies, which had been developing a discourse, have recently clammed up:

> The big factor in the last few years has been the rash of leak prosecutions, as you know, depending on how to define them, three cases where people were prosecuted in leaking classified information in all US history, up to 2009. Since 2009 there have been seven, I believe. That has an enormous impact on people's willingness to talk.

Electronic evidence

Technology provides new tools for government to track down confidential sources. Shane cites the case of Stephen Kim, a State Department official pleaded in guilty in 2014 to leaking information to James Rosen, the Fox News correspondent whose beat included the State Department. It had been revealed in 2013 that the Justice Department had monitored Rosen's activities by tracking his visits to the State Department building, through phone traces, timing of calls and his personal emails in a probe regarding possible leaks of classified information in 2009 about North Korea. Shane observed that while the two men seem to have used the old counter-surveillance method of face-to-face meetings, according to the indictment the Justice Department used electronic records of the use of phone calls and their State Department entry cards to build circumstantial evidence that they were both leaving the building at the same time in the working day and for the same length of time and must have been conducting an unauthorised meeting. The case also has another sinister development. In the indictment the Justice Department described Rosen as a "criminal co-conspirator" with Stephen Kim. In an editorial the *New York Times* said:

> With the decision to label a Fox News television reporter a possible "co-conspirator" in a criminal investigation of a news leak, the Obama administration has moved beyond protecting government secrets to threatening fundamental freedoms of the press to gather news (NYT, 2013).

Another case featuring the prosecution of a journalist's intelligence inside source was of an American lawyer and former CIA employee Jeffrey Sterling who was arrested, charged, and convicted of violating the Espionage Act for revealing details about a botched CIA operation against Iran to *New York Times* journalist James Risen. In May 2015, Sterling was sentenced to 3½ years in prison. Norman Solomon was one of the few reporters to attend all of the Sterling trial and was concerned the successful prosecution rested entirely on circumstantial evidence. He points out those prosecutors made effective use of metadata, which showed that communication took place between Sterling and Risen with the content almost entirely unknown.

> That a prosecution case could be successfully built around such evidence—merely showing that the defendant had communicated with a reporter—should have been alarming to journalists across the country. But news organizations and the big press-freedom groups weren't paying attention to the ominous implications (Solomon 2016).

In Auckland, New Zealand in October 2014, five police officers raided investigative journalist Nicky Hager's home – another interviewee - with a search warrant and spent ten hours looking for information. The purpose of the search was to try and find out the identity of the hacker Rawshark, who hacked into a political analyst's emails and other material on which Hager's then recently published book *Dirty Politics* was based. The book revealed that the prime minister John Key and officials were covertly colluding with bloggers in a major dirty tricks programme, smearing and discrediting political opponents and critics of the governing Party. The police took away Hager's computers, hard-drives, phones, CDs, an iPod

and a camera. These and other cases reveal the threat posed by the collection of metadata to journalists' sources. The raid was later deemed unlawful by the courts. In the UK there have been extensive examples of the police using the Regulation of Investigatory Powers Act 2000 (RIPA) law to covertly examine journalists' phone records to establish contacts with sources.

In the United States about two-thirds of investigative journalists surveyed by Pew believed that the U.S. government has probably collected data about their phone calls, emails or online communications. 80% believe that being a journalist increases the likelihood that their data will be collected. Those who report on national security, foreign affairs or the federal government are particularly likely to believe the government has already collected data about their electronic communications (71% say they believed this is the case) (Pew 2015). There has been relatively little academic discussion on the interrelationships between intelligence and the news media (see Lashmar 2013b; Bakir 2015). Little academic discussion of the impact of Snowden revelations has reached academic journals and has so far taken place in more informal settings, primarily in the media (see Lashmar 2013a, Ponsford 2014). Although the Snowden revelations are still relatively recent there have been some academic texts (Haim 2015; Backman et al 2015; Mols 2015). The impact on journalists covering national security is an important area for research.

In his 2015 report the UK Independent Reviewer if Terrorism Legislation said that documents from Snowden were published "purporting to describe various capabilities of the NSA and other agencies" (Anderson 2105, 22). The author's research has sought to establish the veracity of the documents including consultations with experts such as UK investigative journalist Duncan Campbell[10], former NSA senior executive William Binney[11] and others. They confirm that the Snowden documents are authentic. Some documents from the non-US agencies sometimes exaggerate the effectiveness of their agency and are likely pitched to impress NSA staff. Interpretation continues three years on to ascertain the range of programmes and technologies that are used by the Five Eyes network.

Methodology

The research for this paper utilised several methodologies. First a literature review was undertaken encompassing texts from primary sources, secondary sources and academic texts from Journalism Studies, Intelligence Studies, Surveillance Studies, opinion articles and journalistic texts from authoritative commentators. The Literature Review above concentrated on texts relating to journalists' sources. Other texts are considered and quoted as appropriate in the paper.

Second, the author engaged in reflexive practice based on personal experience to interrogate the possible implications of the Snowden exposures as an investigative reporter, who has handled a considerable number of confidential sources and has reported extensively on intelligence over several decades. The use of reflexive, reflective or transformative practice as a pedagogic tool to improve academic practice has developed since the 1970s (see: Schön 1983, Kolb, 1984, Prpic 2005). Prpic outlines a model for reflexive practice designed specifically for academic practitioners' environment (2005). This reflection results in some of the comments included on the Snowden revelations and also the questions put to the experienced investigative journalists and journalism academics from the Five Eyes countries.

Third, using the research strategy, semi-structured interviews were conducted with experienced journalism practitioners from Five Eyes nations to gauge the impact of the

Snowden revelations on their practice. Semi-structured interviews are a well-regarded qualitative tool and those recorded for this paper were conducted to "obtain descriptions of the life world of the interviewee with respect to interpreting the meaning of the described phenomena" (Kvale 1996, 6). The semi-structured interview approach has been used to good effect as a research tool notably by Aeron Davis (2009) on political journalist-source relations and Damien Tambini (2010) on financial journalists. The interviewees for this paper were chosen on the basis of several interlocking criteria. Snowden's documents are concerned with the Five Eyes countries and the surveillance capabilities of those countries. It was therefore appropriate to interview journalists from these nations. The journalist sub group who are most likely to be affected by the advanced Government/Intelligence Agency capability to identify sources are investigative reporters. The U.S. intelligence academic Loch K. Johnson[12] commented on the role of the media in ensuring accountability of intelligence:

> I think that - in the United States at least - the media has done much more than any other organization or group to advance intelligence accountability. Especially investigative journalists, in their drive for a good story that might lead to their professional advancement and honors (Pulitzers and Polks, for example), have been successful in sniffing out stories and alerting elected overseers in Congress to carry out investigations (2015).

Accountability and oversight

Analysis of oversight investigations of the intelligence community historically reveals those investigations to have been conducted primarily by investigative journalists, usually with prior experience of national security reporting, as it requires exceptional tradecraft and sources. Therefore the author identified investigative journalists who had considerable experience of national security oversight journalism. It is worth noting while journalistic contact with intelligence agencies has traditionally been limited there are and have always been journalists who have contact with these agencies. Access to agencies varies in the Five Eyes countries. In the UK, there are "urinal" journalists that the agencies leak to, in order to spread anonymised information that intelligence agencies would like to see propagated.[13] There are also "accredited reporters" the journalist who acts as a bridge between the agency and their news organisation and who have access to liaison officers within the intelligence agencies (see Lashmar 2013b). The BBC is believed to have four but most major news organisations have one. These formal arrangements mean that the journalist is very much in a "specialist reporter" role. Inherent problems of this arrangement were spelt out by former editor of *The Guardian* Peter Preston "And the trouble with security correspondents is that your prime sources (intelligence agencies) are there in the shadows, always willing and able to pull your strings" (2016). Some Five Eyes' agencies do not welcome formal press approaches.

Criteria for selection

The author sought to interview at least two journalists from each of the Five Eyes countries who met the criteria. Emails were sent to more than twenty journalists and some did not respond. Wendy Bacon, an Australian investigative journalist who is now an academic did not feel she was up-to-date and enabled the author to contact two other suitable journalists. The third of the Australian journalists the author contacted, Dr Phillip Dorling, had experience within government and brought a slightly different yet critical analysis to bear. Also interviewed was the noted Canadian intelligence academic Reg Whitaker[14] who had experience of being in government and close to intelligence. Fourteen interviewees responded

including Whitaker. One journalist did not express any opinion on Snowden pertinent to this paper choosing to discuss impacts on tradecraft only.[15] All those interviewed had at least thirty years of relevant experience on which to base their world view and had worked in the national news media. The twelve journalist interviewees were asked to consider the impact on journalism of the Snowden documents release. The author used semi-structured interviews that considered the participant's experience and career supported by their writings to create a small scale ethnographic survey. The author decided that structured interviews would be too rigid given that while the interviewees had common characteristics their experiences were diverse. For example, some interviewees were no longer writing about national security, others had not dealt with national security or sources since the Snowden revelations. The interviews were conducted by phone and Skype except in one case where Skype was not available and a subsequent interview took place face to face. All interviews were recorded and detailed notes made. Interview times varied from 30 minutes to 90 minutes. In some cases there were supplementary emails, additional short interviews and several one to one meetings. The questions sought to establish the individual's career record as an investigative journalist, which news organisations they had worked in, experience of confidential sources, reporting of intelligence agencies including exposes of intelligence agency practice. It is the author's belief that the answers received were truthful and accurate as any provided by recollection can be. The author's background and reasons for the interview were explained to each interviewee and informed consent was given to use their quotes except where explicitly stated by the interviewee. I have not made use of any off-the-record comments. Interviewees were aware of my journalistic background. The author had prior acquaintance with two of the UK interviewees and had contact in the past with one of the US interviewees. Other journalists, academics, intelligence practitioners and commentators and have been quoted from secondary sources where appropriate to compare and contrast.

Results

Shock of the scale of mass surveillance

No interviewee disputed the value of good intelligence in the interests of national security. The UK investigative journalist, a specialist writer on electronic intelligence and interviewee Duncan Campbell[16], pointed out that that the Five Eyes operational network does now perform the anti-terrorism role well:

> They are doing effective anti-terrorism. It does work. It's what people want. It's what journalists absolutely do not seek to expose and that is shown in the Snowden case which is dripping with this stuff that I doubt will ever see the light of day because it is about anti-terrorism.

While experienced investigative journalists have long known that the intelligence agencies had the ability to surveil them, the interviewees have been astonished by the quantity of data that is being taken by the Five Eyes agencies. That so much communications data is stored by the agencies and available for retrospective analysis and as potential evidence for seeking warrants and indictments was also a shock. Australian investigative journalist, Philip Dorling[17], who has also worked in government and politics, said: "Edward Snowden's revelations about the mass acquisition of telecommunications data and bulk interception of internet traffic by the US National Security Agency provide a salutary warning of how technological change has developed the architecture for a surveillance state". In the US more law enforcement actions against reporters covering national security and their sources have

been instigated under the Obama Presidency than any previous administration. Interviews with practitioners and academics for this paper revealed arrange of approaches to the post Snowden issues of protection of sources as an ontological problem, a question of risk analysis, or a journalism practice issue. Interviewee Christopher Hird[18], was until 2015 was editor of the *Bureau for Investigative Journalism,* said the Snowden revelations will have a big impact on journalist and source practice:

> You have to work on the assumption that if the authorities decide to take an interest in you they will be able to discover nearly anything you are up to, who you are meeting, what research you are doing, who you are talking to and what your networks are. If they so choose it is relatively easy for them to do, and confirms the suspicion one has had for some time, particularly in the digital world, one has to understand it is easier for them to do this than in the past.

Hird, citing the arrest of journalists Duncan Campbell, Crispin Aubrey and former Signals Regiment soldier John Berry under the UK's Official Secret Acts (OSA) in 1976, points out the authorities have had the ability to monitor journalists' communications for a long time.

> But, it is now less hit and miss. What both the Snowden and to some extent the Julian Assange affair have demonstrated is that states are among the greatest enemies of free open expression and accountable government. In the practical sense that is much more concerning now than it was in the 1970s.

Gavin MacFadyen[19], director of the UK Centre for Investigation Journalism (CIJ) and points out that some mainstream press media support greater surveillance powers for government. Snowden, he said, has exposed "more dramatically than any us we would have ever expected…the inadequacy of the mainstream press, its embarrassing proximity to power and its refusal to embarrass power on the whole. Andrew Fowler[20], a former correspondent for ABC *Four Corners* current affairs TV programme, observed: "The internet has actually opened everything up but at the same time has given the state much more power and enabled them to see every move we make." The extent that agencies within the Five Eyes group are prepared to go to breach lawyer's confidentiality is shown by the East Timor bugging scandal in Australia (see Allard 2013, Toohey 2013). Duncan Campbell[21] counselled it was important to keep things in perspective and only a relatively small number of journalists are likely to run up against surveillance by the NSA network:

> The impact of Snowden's revelations should not really be overstated for journalism, because the most critical aspect relates to the conduct of the intelligence.

He added:

> There are a huge number of stories, from tracing contamination in food to medical scams to corruption in business, where there's not the remotest possibility that the extensive capability of NSA and GCHQ, and those they share with, is not going to be allowed anywhere near those [journalists] who might seek to interdict the source of this journalism.

The *New York Times* and interviewee journalist Scott Shane[22] observes that contemporary electronic data from phones and other technology enables the tracking of journalists and their sources. He said in the past with FBI leak referrals the first thing they did was fill in a questionnaire as to how many people were cleared for the information: "And it would be giant numbers say 200 or 5000, essentially too big and the FBI would shrug its shoulders.

That's changed." Shane describes the way American officials now track down leakers. They are not looking for primary evidence in the first instance, but evidence of knowledge and prior contact:

> It's not that that your sources in the national security world sends you an email saying "Dear Scott, here's the secrets you were asking about", it's that they see your story in the newspaper, at NSA or CIA or whatever, they say "ah ha, Scott Shane". They put "Scott Shane" into their government email system and they say "Ah ha, Scott Shane has exchanged emails with these seven people in our agency in the last five years. Two of them he has been in touch with recently. But first of all of those seven people, who of those know about this topic? Oh, two of them know about the topic."

Therefore tracking down sources is much easier and Shane observed many potential sources are deterred by leak prosecutions.

Lack of intelligence accountability

The Snowden surveillance debate is focussed on metadata as no examples have been revealed of actual data from within those communications being used against journalists. The documents do reveal large scale specialist hacking operations into target computers especially by the NSA"s Tailored Access Operations (TAO) group - a cyber-warfare unit (Walters 2013). There has been one ominous glimpse of the potential of Five Eyes hackers to intercept and use journalist's private communications. According to *Der Spiegel*, the NSA hacked the computers of Al-Jazeera journalists in Qatar in search for terrorism contacts. One such document, dated March 23, 2006, revealed that the NSA's Network Analysis Center managed to access and read communication by "interesting targets" that were specially protected by the news organization (Der Spiegel 2013). If eavesdroppers are able to identify sources and locations of sources from within the private computers in news organisations, this has serious ramifications. Journalists may well have contacts in terrorist groups as a legitimate part of their work. But what happens if their contacts are hacked, identified and eliminated? How should journalists react if they now know that a source may be tracked and say, killed in a drone attack, because eavesdropping agencies have broken into "secure" communications? Observing that the Five Eyes countries also have a wider partial sharing network with another 35 partner countries, Duncan Campbell[23] believes that in the post 9/11 world intelligence agencies have been given unprecedented resources and latitude but the oversight has not kept pace:

> There are not remotely enough safeguards in place. Most national parliaments have no idea what is going on. There are two sets of poisons running here: the British-American alliance and the secret influence that has and then a global "little brother" network [the 35 other national partners]. These agencies have their own agendas and the release of many constraints after 9/11 just means they flourished like a cancer and the growth means they are not fit for purpose.

Campbell cmmented that the problems journalists are discussing are "much more psychological than about electronics" and that tradecraft in handling sources is important. He also points out that journalists needed a better understanding of who sets intelligence requirements for GCHQ when it comes to monitoring an individual's communication and thus which journalists and sources are realistically likely to be at real risk of state eavesdropping of their messages.

Government reaction

David Fisher[24], a *New Zealand Herald* journalist who covers national security and interviewee, said that one of the benefits of the Snowden Affair is that the New Zealand government under Prime Minister John Key has improved the oversight of its intelligence agencies:.

> John Key has opened up the spy agencies to public scrutiny in a way which we have never seen in New Zealand. We know more now about what they do and even how they do it. We know how the two agencies are managed, in that the GCSB and NZSIS both have top-flight lawyers in charge.

Canadian journalist Andrew Mitrovica[25] does not believe that new Trudeau Government's post-Snowden oversight response has been adequate. Commenting after the federal government released an oversight annual report at the beginning of 2016 Mitrovica described the oversight agencies: "as tiny, inexperienced, underfunded, easily intimidated, easily befuddled, largely part-time outfits known as the Security Intelligence Review Committee (SIRC) and the Office of the Communications Security Establishment Commissioner" (Mitrovica 2016).

Campbell[26] believes that there is only one effective method to stop total surveillance; "the smartest and simplest way, rather than complexity, is to cut their budgets so they have to cut back to the things they are there to do." Hird[27] said that the information revealed in the Snowden affair is one of a "constellation" of problems facing journalists in protecting their sources. He said that the phone hacking scandal in the UK has made contact much more legally risky in certain circumstances.[28]

> Approached by a police whistle-blower, now instead of arranging to meet that person, the first thing you have to do is seek legal advice to find out whether they are in danger of breaching their contract and whether you are at risk of commissioning a criminal act.

Protecting sources

Of the twelve journalists interviewed all believed that Snowden's revelations of Five Eyes powers of surveillance raised issues of major concern over the ability of journalists to protect sources. Fowler[29] said that Snowden has made a lot of difference. "I could never guarantee to a source that I could protect them but I would tell them what I would do to protect them." He said he never had a source identified and prosecuted. "I prefer to lose a story than lose a source." He observed it is much more difficult post Snowden and that it was not journalists that are affected: "I recently addressed a conference of accountants in Perth about this very issue. They were somewhat staggered by all of this."

Several interviewees, for example Christopher Hird[30], as seen above, questioned whether we could protect sources at all. Gavin MacFadyen[31] of the CIJ argued that the Snowden revelations meant the ability of journalists to protect sources is now critical: "There has never been anything like this, except in the worst totalitarian states, compared to the threat to free inquiry now". He believes everything changed with Snowden and journalism will not be same. "No, never" he said. Interviewee Brian Toohey[32], an Australian journalist specialising in electronic intelligence issues and a former editor of the *National Review,* cites ASIO's interception and subsequent raid in 2013 on an Australian lawyer's practice communications who were acting on behalf of the East Timorese as an example of the increased surveillance and intervention capability of Australian intelligence and law enforcement agencies (Toohey

2013). The American intelligence writer and interviewee, Jeff Richelson[33], said that the threat of journalists not being able to protect sources, particularly those reporters covering the overlapping areas of terrorism and intelligence, was very serious. Australia's Andrew Fowler[34] commented:

> It is certainly more significant for journalists covering intelligence, terrorism and policing issues but having said that it is an issue that should concern all journalists. There is, for example, a rather odd culture in Australia, where communications security for journalists was seen before Snowden as being slightly odd-ball. Many did not use simple email encryption systems or TOR[35], though that is now slowly changing

Jeff Sallot[36] , a Canadian national security reporter, now an academic, said it was particularly serious for reporters in the national security sector and we have learned through the Risen case, which began in 2005, that American authorities are not deterred by the First Amendment in their pursuit of leakers.

> Risen's phone was tapped and his emails monitored from an early date. He was later threatened with jail time for contempt for refusing to disclose source identities in a court case. The feds backed off after the jailing of Judith Miller turned a flawed journalist into a Free Press icon. Risen, like Miller, had the backing of a potent media organization. Reporters who don't work for *The New York Times* have to wonder whether in the final analysis their bosses have their back.

Consequences

The New Zealand investigative journalist, who specialises in electronic intelligence and another interviewee for this paper, Nicky Hager[37] does believe he can still protect his sources:

> Because I have worked on sensitive subjects, I would just never leave call data between me and a sensitive source. I'd never e-mail them either. I'd never write something on my computer that could identify them. I have highly encrypted drives and computers and occasionally use PGP[38] (all of these important tools that reduce risks), but for 95% of my work I use open e-mail and phone and I just draw a line around things where someone could be harmed and use low tech methods to leave no traces. Snowden's revelations are a wake-up call for everyone who might one day be targeted. I especially think of the state capacity for hacking which goes beyond what I imagined. But I still believe that the methods I use are viable at present to deal with the technological threats Snowden has revealed.

Canadian investigative reporter Andrew Mitrovica[39] agreed with Hager and believes he can protect sources. But he does not believe that there is any such thing as effective encryption. He noted reports that suggest that many software packages have "backdoors" available to the intelligence agencies. "I think we need to go back to the Watergate module and meet sources in basements and parking lots. We need to revise our communication tradecraft, even use dead letter boxes, avoid, where possible, technology," he observed. Director of CIJ, Gavin MacFadyen[40] believes that journalist must use encryption methods like TOR.

> The notion that this is sort of marginal thing you have an option to do, I think that has been by-passed now. I mean any journalist, who is operating with serious sources, not dealing with travel writing or things like that, and does not use these methods is just inviting catastrophe later. That is how serious it is.

Others believed new tradecraft needed to be developed. MacFadyen believes that the intelligence agencies capabilities "an incredible threat to us, our sources and democratic process. Knowledge is power and we give them all this knowledge without constraint with no fear of perjury." He concludes sceptically: "These people lie all the time." Andrew Fowler[41] says post-Snowden he has started using the encryption software PGP. "I was careful before Snowden but now I am really, really careful." Fowler has recent experience of working with a confidential government source, and points out these sources can make themselves vulnerable:

> Even though they [insider sources] are involved in the intelligence community there is a striking naivety with which they deal with us as professional journalists. We try to protect them. I go through all the things to protect then – not taking phones that sort of thing – then they text me! I raise it and they say 'no, no, it's alright'. No it's not alright

It is clear that most experienced journalists are revising their methods of protecting sources. All the journalists interviewed thought that Snowden's revelations would have a chilling effect on confidential sources speaking to journalists. As Bradshaw stated: "historically, protecting sources has been a *reactive* process: one that only begins *after* the contact has been made (2015, forthcoming). New Zealand journalist David Fisher[42] observed: "It's going to put some people off." He said that, while protecting sources has always been an issue and subject to constant updating of techniques, Snowden has affected the way he deals with potential sources: "I had this funnily enough the other day. I had somebody make contact with me through a private email address. Almost the first thing we talked about is how we were going to communicate in the future." Opening on such an off-putting, but now vital, point is new, said Fisher: "It is a feature in the last six months that we have to go through the 'anonymity and protection' dance before we could get down to business." Scott Shane[43] said: "What you are going to get in effect is people saying 'So you want me to risk going to prison so your story is a bit better'. I don't think so."

Harsh legislation

In each of the Five Eyes country there has been new legislation to either give legality or greater legality to bulk collection by the intelligence agencies or to deter sources leaking information to journalists. At the time of writing the UK the Government is pushing through a revised Investigatory Powers Bill, also known as the "Snooper's Charter mark two" designed to place GCHQ in a stronger legal framework. It brings into one Bill powers encompassed previously in many diverse Acts. UK journalist and interviewee Duncan Campbell[44] observed:

> What is being said to the public and Parliament right in Britain now is 'Trust us' - trust the judges, trust the system - and many people want to. But that we have seen from the record is that over 30-40 years, they cannot be trusted.

Criticised by a range of human rights, civil liberties, journalism and politicians the Government has revised the Bill. Warrants will need judicial rather than political approval. The Bill though legitimises bulk collection and in the assessment of the author lacks effective accountability mechanisms to monitor such an overarching legalisation. Whilst the Investigatory Powers Bill recognises that MPs, journalists and lawyers serve public interest functions, critics believe the Bill does not safeguard the confidentiality of their communications and related activities which underpins those functions. There are similar stories in other Five Eyes countries. Fowler[45] notes that the Australian Government have

legislated to crack down on journalists publishing national security information with the potential of long sentences. He states the Security Forces and Executive Government have taken advantage of Snowden revelations to push through harsh legalisation to make journalism more difficult. "It is exactly what Daniel Ellsberg[46] warned Julian Assange[47] when he [Assange] said to him that he wanted to open governments and make them accountable. And Ellsberg said I think you will find exactly the reverse will happen." Indeed as Fowler and others interviewees noted that the war on terror, now in its second decade of instilling fear into the public, has allowed governments to crack down on journalists and their sources. Glenn Greenwald commented: "This near total capability to access everyone's conversations is justified on the grounds of fighting the 'war on terror' and organised crime" (Greenwald 2013a). Loch K Johnson's proposition 37 from his proposed theory of strategic intelligence seems to apply here: "In times of military crisis, a nation tends to rally behind its leader in favour of an efficient intelligence and military response to the threat, placing at a lower level of concern questions of civil liberties and intelligence accountability" (Johnson 2009, 51).

As Bauman et al pointed out, the implications of the Snowden affair are so major that few have had the opportunity to fully evaluate their potential impact on the political, cultural and public sphere (2014). What is apparent since 9/11 is that most journalists have sleepwalked into a world of mass surveillance where, to all intents and purposes, intelligence agencies have, with dubious legality and ineffective oversight, had access to the electronic communications of anyone who uses mobile phones, computers, credit cards and access ID cards. In the UK this was probably illegal as the Intelligence community has covertly operated under forty plus laws that were never meant to cover metadata collection such as Section 94 of the Telecommunications Act 1984. Much of this legislation was passed into law before modern bulk collection was feasible and was never envisioned by Parliament to provide legality to these activities. Some experts say this was legal, to which the author would respond that it has never been tested in court so we simply do not know. This was neither known to, nor discussed by Parliament and there appears to have been a failure of the official accountability bodies to act. In each of the Five Eyes countries government and intelligence agencies secretly operated without reference to the democratic process. When Snowden's revelations forced their hand to come clean about their activities and request new laws to operate the Intelligence lobby claimed it had been necessary to fight the war on terror. The speed of change is remarkable. Within a few years journalists have gone from a situation where they had a very high percentage guarantee of protecting a confidential source to a situation that they have to assume, at least when it comes to investigations into government, the public sector and related private sectors, the percentage has shrunk.

Conclusions

Snowden's disclosures presents journalists, as other professions with a problem of source protection as their professional ethics require total confidentiality, journalists have to ask whether they are any longer in a position to give that guarantee. In a sense it does not matter whether intelligence agencies do use data to track down confidential sources, it is the fact that they can do so much more easily than ever before that is significant. The negative effect of "chilling" the flow of information from confidential sources was, as we have seen, recognised at least as far back as the Watergate Scandal in the early 1970s. In recent years governments have chosen to turn the temperature control down further. What Snowden disclosed may freeze the flow. The current situation will prevent all but the most determined from speaking to journalists. In effect the threat of mass surveillance may all but eliminate confidential sources. Given that many experienced journalists believe confidential sources were once an effective accountability mechanism, few think that internal accountability

remedies work, and that much of government and related private sector organisations will no longer subject to effective scrutiny by the fourth estate.

This paper's main conclusion is that the ambition of the NSA network to store huge swathes of global communications data does take the world into a new surveillance paradigm and there is an existential change in the nature of relationships between journalists and confidential sources. This paper also concludes that this debate is still live, with journalists and academics still considering the implications. As we have seen the views range from the apocalyptic to the pragmatic but the general consensus is that Snowden has serious implications for journalism, also for other professions where ethics of confidentiality are central, but more importantly for democracy. It is also apparent that with the current levels of terrorism, the large swathes of the publics of the Five Eyes countries are prepared to sacrifice some civil liberties, including press freedoms, in return for a social contract that appears to offer greater security. Journalists will not, of course, give up but what are they to do? They can take the "open plan" approach of hiding sources in plain sight. But that is a high risk strategy. Most interviewees suggest that a much improved tradecraft for protecting sources is needed. In addition journalists need to be more outspoken about the impact of surveillance in preventing them from delivering their most important role, bringing to account government and the powerful when they are errant.

Documents released from the Snowden cache indicate that intelligence agencies operate on a hitherto unexpected, global capability of penetration and coverage, with both defensive and aggressive remit. It is also clear that the formal accountability systems for intelligence services are woefully inadequate in all the Five Eyes countries. At a time when the news media, more than ever, needs to exert scrutiny over the burgeoning intelligence community with their expanded capacity and licence to spy and intrude, unfortunately coincides with a new era where the agencies' fast developing technological capability enables them to deter public interest inquiry.

---

[1] At the time of writing some 6000 of these documents had entered the public domain.
[2] Metadata is defined the data of data and in this case is information that accompanies and individually defines emails, phone calls, texts and other electronic communications but is not the content data.
[3] The author of this paper read the Agee's book in 1976 then met and interviewed Phil Agee in 1977.
[4] Search terms used included 'Snowden', 'Greenwald', 'Poitras', 'journalism and sources', 'confidential and sources', 'journalist and sources', 'anonymous and sources'.
[5] The impact of Snowden's material on whistle-blowers will be dealt with in a subsequent paper.
[6] Dorling is former political adviser, commentator, former government adviser and investigative journalist in Australia.
[7] Deep Throat is the pseudonym given to the confidential source who provided information to Bob Woodward and Carl Bernstein of The Washington Post in the early 1970 in what came to be known as the Watergate scandal.
[8] Fowler. Interview. 10 September 2013.
[9] Shane. Interview. 17 December 2013.
[10] Campbell. Interview. 2 January 2014 and follow up communications.
[11] Binney. Personal communication. 5 March 2016.
[12] Johnson. Personal communication. 23 February 2013.
[13] The derogatory expression 'urinal journalist' was first applied to Chapman Pincher of the Daily Express. Pincher's journalism has always been controversial and in the 1960s he was the target of historian E.P.Thompson's famous caustic observation that, Chapman was 'the urinal where Ministers and officials queued up to leak to'. Urinal journalism is now taken to mean stories based on leaks from government sources who want to spread disinformation or settle Whitehall scores.
[14] Whitaker also wrote *The End of Privacy: How Total Surveillance Is Becoming a Reality* (1998)
[15] The author also asked questions to interviewees where appropriate about professional practice to protect sources which is for a subsequent paper.

[16] Campbell. Interview. 2 January 2014 and follow up communications.
[17] Dorling. Interview. 15 January 2014
[18] Hird. Interview. 23 December 2013.
[19] MacFadyen. Interview. 2 January 2014.
[20] Fowler. Interview. 10 September 2013.

[21] Campbell. Interview. 2 January 2014 and follow up communications.
[22] Shane. Interview. 17 December 2013.
[23] Campbell. Interview. 2 January 2014 and follow up communications.
[24] Fisher. Interview. 21 November 2013.
[25] Mitrovica. Interview. 6 September 2013.
[26] Campbell. Interview. 2 January 2014 and follow up communications.
[27] Hird. Interview. 23 December 201.3
[28] Phone hacking is major journalism scandal in the UK. Journalists from the News of World were hacking voicemails or a wide range of people for the purposes of stories. The scandal has been detrimental for Rupert Murdoch the owner of the tabloid News of the World, who shut the paper down in wake of the exposure. A number of prosecutions are underway at time of writing. The scandal has spread to other news organizations and has also revealed payments to public officials.
[29] Fowler. Interview. 10 September 2013.
[30] Hird. Interview. 23 December 2013.
[31] MacFadyen. Interview. 2 January 2014.
[32] Toohey. Interview. 30 December 2013.
[33] Richelson. Interview. 10 October 2013.
[34] Fowler. Interview. 10 September 2013.
[35] TOR is open software for enabling anonymous communication. The name is an acronym from the original software project name The Onion Router.

[36] Sallot. Interview. 10 September 2013.
[37] Hager. Interview. 31 December 2013.
[38] Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.

[39] Mitrovica. Interview. 6 September 2013.
[40] MacFadyen. Interview. 2 January 2014.
[41] Fowler. Interview. 10 September 2013.
[42] Fisher. Interview. 4 November 2013.
[43] Shane. Interview. 17 December 2013.
[44] Campbell. Interview. 2 January 2014 and follow up communications.
[45] Fowler. Interview. 10 September 2013.
[46] Daniel Ellsberg leaked the 'Pentagon Papers' that revealed the United States of America was losing the Vietnam War.
[47] Julian Assange is the founder of WikiLeaks

References

Agee, Phil. 1975. *Inside the Company, CIA Diary.* London: Penguin Books.

Allan, Stuart. (ed). 2005. *Journalism: Critical Issues*. London: Open University Press.

Allard, Tom. 2013. "ASIO raids office of lawyer Bernard Collaery over East Timor spy claim". *Sydney Morning Herald*. http://www.smh.com.au/federal-politics/political-news/asio-raids-office-of-lawyer-bernard-collaery-over-east-timor-spy-claim-20131203-2yoxq.html#ixzz2qqhs1X44 December 3.Arar Inquiry: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher

Anderson, David. (2015). *A Question of Trust: Report on the Investigatory Powers Review*. Can be downloaded from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf

Arar 2006. http://www.sirc-csars.gc.ca/pdfs/cm_arar_bgv2-eng.pd.

Backman, Christel., Johnson, Erica,. Saetnan, Ann., Rudinow, Toendel, Gunhild., Svenonius, Ola. and Wigorts Yngvesson, Susanne. 2015, "Post-Snowden Surveillance Journalism in Scandinavia." paper presented to Surveillance and Citizenship: State-Media-Citizen Relations after the Snowden Leaks, Cardiff University, June 18-19

Bakir, Vian. 2015. "News, Agenda Building, and Intelligence Agencies: A Systematic Review of the Field from the Discipline of Journalism, Media and Communications." *The International Journal of Press/Politics* 20 (2): 131-144.

Bauman, Zygmunt., Bigo, Didier., Esteves, Paulo., Guild, Eslpeth., Jabri, Vivenne., Lyon, David. and Walker. R.B.J. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8: 121–144.

Bradshaw, Paul. 2015. "Chilling effect: regional journalists' source protection and information security practice in the wake of the Snowden and RIPA revelations". Forthcoming.

Broersma, Marcel,. den Herder, Bas. and Schohaus, Birte. 2013. "A question of power." *Journalism Practice* 7-4: 388-395.

Campaign for the Protection of Journalists (CPJ) 2013. *CPJ's recommendations to the Obama administration.* https://cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911-recommendations.php

Campbell, Duncan. 2016. "The Snooper's Charter: A threat to Press Freedom? *Listening Post* programme, Al-Jazeera. http://www.aljazeera.com/programmes/listeningpost/2016/01/uk-snoopers-charter-threat-press-freedom-160124101711356.html. January 24.

Carlyle, Thomas. 1840. *On Heroes, Hero-Worship, and the Heroic in History*. http://www.gutenberg.org/files/1091/1091-h/1091-h.htm.

Carlson, Matt. 2012. *On the Condition of Anonymity* Chicago: University of Illinois Press.

Corera, Gordon. 2015. *Intercept: The Secret History of Computers and Spies.* London: Weidenfeld & Nicholson

Cottle, Simon. 1998. "Ulrich Beck, 'Risk Society' and the media, a catastrophic view?" *European Journal of Communication* 13 (1):. 5-32.

Crook, Tim. 2003. "Is Your Source Ever Really Safe?" in *British Journalism Review* 14: 7.

Davis, Aeron. 2009. "Journalist – source relations, mediated reflexivity and the politics of politics." *Journalism* Studies 10 (2), 204-219.

Der Spiegel. 2013. "Snowden Document: NSA Spied On Al Jazeera Communications" in *Der Spiegel*. http://www.spiegel.de/international/world/nsa-spied-on-al-jazeera-communications-snowden-document-a-919681.html August 31.

Dorling, Philip. 2012. Transcript of talk by Dr Philip Dorling from the Freedom of information panel discussion for Recordkeeping Roundtable held in Sydney on February 29 2012. http://rkroundtable.org/2012/03/24/philip-dorling/

Dorling, Philip. 2013a. “Living in a state of surveillance”. *The Melbourne Age*.. Can be seen at http://www.theage.com.au/it-pro/security-it/living-in-a-state-of-surveillance-20130612-2o4au.html June 13

ECHR, 1996. *Goodwin v. United Kingdom.* http://hudoc.echr.coe.int/eng?i%3D001-57974#{"itemid":["001-57974"]}

Fisher, David. 2015. “Just how bad were our spies?” *New Zealand Herald.* 6 Nov 2015. This http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11541220 February 6.

Gans, Herbert. 1980. *Deciding What’s News*. London: Constable.

Greenberg, Sue., 2007. “Theory and practice in journalism education.” *Journal of Media Practice*. 8 (3): 289-303.

Greenwald, Glenn., MacAskill, Ewen. and Poitras, Laura. 2013a. "Edward Snowden: the whistle-blower behind the NSA surveillance revelations.” *The Guardian* (London). http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance June 9.

Greenwald, Glenn. 2013b. “The NSA Can ‘Literally Watch Every Keystroke You Make.” *Democracy Now*.. http://www.democracynow.org/2013/12/30/glenn_greenwald_the_nsa_can_literally December 30.

Greenwald, Glenn. 2015. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State.* London: Penguin.

Haim, Mario 2015, ‘Resetting the Agenda? NSA Coverage in Traditional and New Online Media’, paper presented to Surveillance and Citizenship: State-Media-Citizen Relations after the Snowden Leaks, Cardiff University, June 18-19.

Hall, Stuart., Critcher, Charles., Jefferson, Tony., Roberts, Brian. and Clarke, John., 1978. *Policing the Crisis, Mugging, the State and Law and Ord*er. London: Palgrave Macmillan.

Hallin, Daniel C., Manoff, Robert. Karl., and Weddle, Judy K. 1993. “Sourcing patterns of National security Reporters,” *Journalism Quarterly* 70.

Hamilton, John Maxwell. & Tworek, Heidi J S. (2016) “The natural history of the news: An epigenetic study,” *Journalism,* Online First:. January 28. London: Sage.

Harding, Luke. 2014. *The Snowden Files: The Inside Story of the World's Most Wanted Man.* London: Guardian Faber Publishing.

IFJ, 1986. *International Federation of Journalists Declaration of Principles on the Conduct of Journalists*. http://www.ifj.org/about-ifj/ifj-code-of-principles/.

Johnson, Loch K. 2009 “A Theory of Strategic Intelligence.” In Gill, Peter., Marrin, Stephen. and Phythian, Mark. (eds) *Intelligence Theory: key questions and debates.* Abingdon: Routledge.

Johnson, Loch K. 2015. Correspondence with author. February 23.

Kiernan, Matthew. 2000. “The Regulatory and Ethical Framework.” In de Burgh, Hugo. (ed) *Investigative Journalism: Context and Practice.* Oxford: Routledge 1st ed.

Kolb, David A., 1984 *Experiential learning: Experience as the source of learning and development.* New Jersey: Prentice-Hall.

Kvale, Steiner. 1996. *Interviews - An Introduction to Qualitative Research Interviewing.* London: Sage.

Lashmar, Paul. 2013a. “No More Sources.” *Open Democracy*, 2015. https://www.opendemocracy.net/paul-lashmar/no-more-sources October 17.

Lashmar, Paul., 2013b ‘Urinal or open channel? Institutional information flow between the UK intelligence services and news media.’ *Journalism: theory, practice and criticism*. Published online January 30. London: Sage.

Lashmar, Paul. 2015. *Investigating the ‘Empire of Secrecy’ — three decades of reporting on the Secret State.* PhD thesis. Brunel University.

Luckhurst, Tim. 2003. “Nowhere to Hide” *The Independent*. http://www.independent.co.uk/news/media/nowhere-to-hide-97229.html July 22

Lyon, David. 2015. *Surveillance After Snowden*. Bristol: Polity Press.Manning, Paul. 2001. *News and News Sources*. London: Sage.

Manning

Mitrovica, Andrew. 2004. “RCMP Follies.” *Media*, Spring 2004. 10. (3): 6-7. Pub by the Canadian Association of Journalists. http://caj.ca/wp-content/uploads/2010/mediamag/awards2007/Andrew_Media_spring_2004.pdf. Mitrovica, Andrew. 2016. “Think the Liberals will rein in the spy services? Don’t bet money on it.” *iPolitics*. http://let.snowden.in/2016/01/30/think-the-liberals-will-rein-in-the-spy-services-dont-bet-money-on-it-ipolitics-20160129/ January 30.

Mols, Anouk. 2015, ”Not Interesting Enough to be Followed by the NSA': A Frame Analysis of the Dutch Public Debate About the NSA Revelations in 2013”, paper presented to Surveillance and Citizenship:State-Media-Citizen Relations after the Snowden Leaks, Cardiff University, June 18-19.

Moran, Christopher. (2013) *Classified: Secrecy and the State in Modern Britain*. Cambridge: Cambridge University Press.

New York Times. 2013. “Another Chilling Leak Investigation” Editorial. http://www.nytimes.com/2013/05/22/opinion/another-chilling-leak-investigation.html?_r=0 May 21.

O’Carroll, Lisa. 2013. “Seymour Hersh on Obama, NSA and the 'pathetic' American media. *The Guardian.* http://www.theguardian.com/media/media-blog/2013/sep/27/seymour-hersh-obama-nsa-american-media September 27.

Park, Robert E. (1923) “The Natural History of the Newspaper.” *American Journal of Sociology*. 29(3): 273-289.

Parrell, Mark J. 1993. “Press/Confidential Source Relations: Protecting Sources and the First Amendment.” *Communication and the Law*. 15 47-73.

Pearlstine, Norman. 2007. *Off the Record: The press, the Government, and the War over Anonymous Sources*. New York: Farrar, Straus and Giroux.

Pew Research Center in association with Columbia University's Tow Center for Digital Journalism, 2015, "Investigative Journalists and Digital Security". February 5

Pincher, Chapman. (2009) “Reflections on a Lifetime of Reporting on Intelligence Affairs.” In Dover, Robert. and Goodman, Michael S. (eds). *Spinning intelligence: Why Intelligence needs the media, Why the media needs intelligence.* London: Hurst & Co.

Ponsford, Dominic. 2014. “Rusbridger on how no journalist's sources are safe, joining IPSO and why he would have kept News of the World open”. *Press Gazette*.. http://www.pressgazette.co.uk/rusbridger-how-no-journalists-sources-are-now-safe-joining-ipso-and-why-he-would-have-kept-news/ March 28.

Ponsford, Dominic. 2015 *“News Corp and Trinity Mirror need to address betrayal of sources if industry is to move on from hacking scandal.” Press Gazette*. http://www.pressgazette.co.uk/content/67-british-journalists-arrested-andor-charged-course-their-jobs-2011 December 11.

Preston, Peter. 2016. “Beware spooks stringing along security reporters”. *The Guardian,* http://www.theguardian.com/world/2016/jan/10/beware-spooks-stringing-along-security-correspondents.January 10..

Prpic, J Kaya, (2005) “Managing academic change through reflexive practice: A quest for new views”. *Research and Development in Higher Education* 28, 399-406.

Reich, Zvi. 2008. “The Anatomy of Leaks.” *Journalism* October 2008 9 (5): pp 555-581

Sager, Kelli L, and Wilcox, Rochelle L. 2007. “Protecting Confidential Sources.” In *Litigation* Winter 2007: 33 (2): 36-41.

Schlesinger Philip, 1990. “Rethinking the Sociology of Journalism: source strategies and the limits of media-centrism.” In Ferguson, Majorie, *Public Communication: the new imperatives*. London: Sage.

Schlesinger, Philip. and Tumber, Howard. 1994. *Reporting Crime*, Oxford: Clarendon

Schön, Donald. (1983) *The Reflective Practitioner*. London: Temple Smith

Sigal, Leon. 1973. *Reporters and Officials*. Lexington, MA: D. C. Heath.

Solomon, Norman. 2016. “Should journalists care if sources go off to prison?” *Columbia Journalism Review*.. http://www.cjr.org/opinion/should_journalists_care_if_sources_go_off_to_prison.php L February 5.

Stein, Jeff. 2013. “The End of National Security Reporting?” *Computer Security*. http://www.computer.org/cms/Computer.org/ComputingNow/pdfs/TheEndOfNationalSecurityReporting-IEEESecurityAndPrivacy.pdf July/August

Tambini, Damian, 2010. What are financial journalists for? *Journalism Studies* 11 (2): 158-174.

Toohey, Brian. 2013. "Attorney-General George Brandis wades into troubled waters." *The Financial Review*. . http://www.afr.com/news/policy/foreign-affairs/attorneygeneral-george-brandis-wades-into-troubled-waters-20131206-iypc7 December 7.

Walters, Joanna. 2013. "NSA 'hacking unit' infiltrates computers around the world – report." *The Guardian.* December 29.

Whitaker, Ray., Lashmar, Paul and McSmith, Andy. 2003. "Revealed: How Blair used discredited WMD "evidence": UK intelligence chiefs warned claim that Iraq could activate banned weapons in 45 minutes came from unreliable defector." *The Independent on Sunday*, June 1.

Journalist interviewees:

Australia: Andrew Fowler;

Brian Toohey

Dr Philip Dorling,

Canada: Andrew Mitrovica;

Jeff Sallot.

New Zealand: David Fisher, Nicky Hager,.

UK, Duncan Campbell, Christopher Hird

Gavin MacFadyen,

US: Scott Shane,

Jeff Richelson,

Disclosure statement

I received no grant funding for this publication. I am part of a current research group DATA PSST! That is investigating privacy and surveillance issues that is funded by ESRC and have been part of a research team that received a grant from Innovate UK (2014) but not on a subject area related to this article.